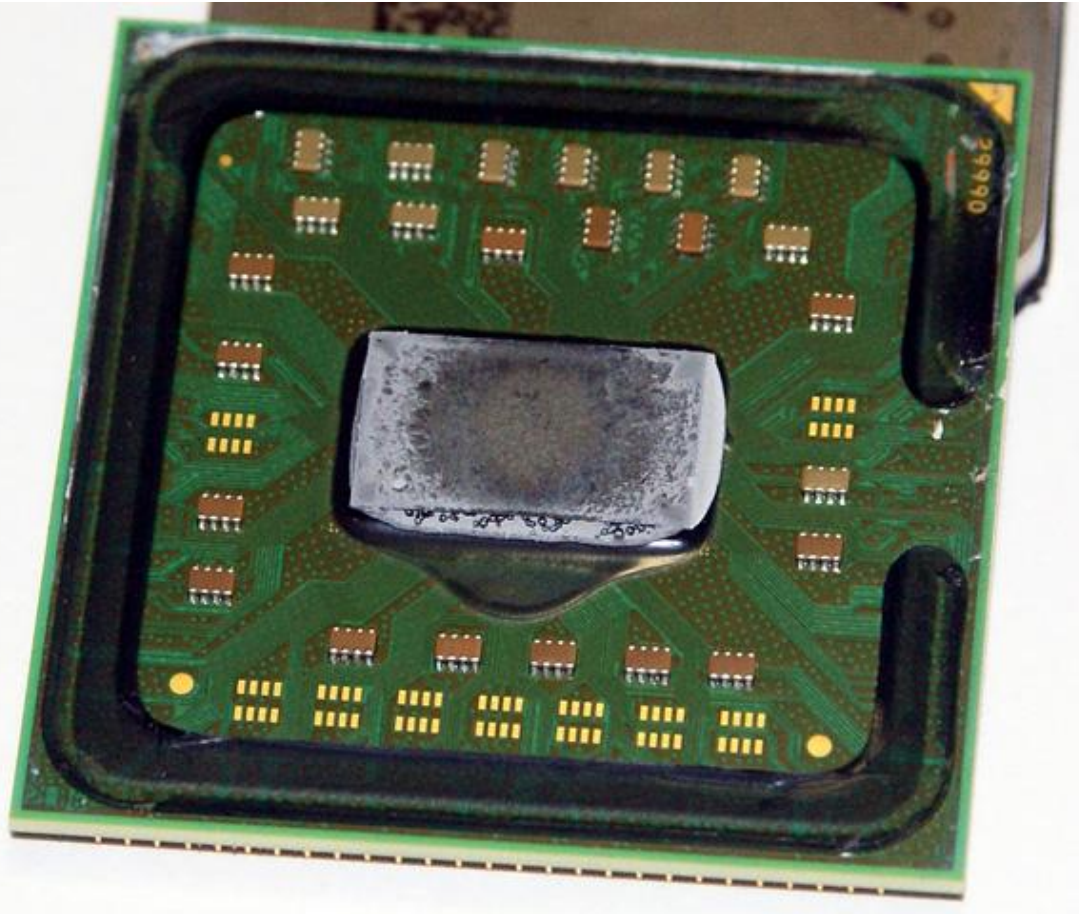


Технологии тепловой и
антивирусной защиты;
энергосбережения.

Охлаждение ЦП



Тепловая защита



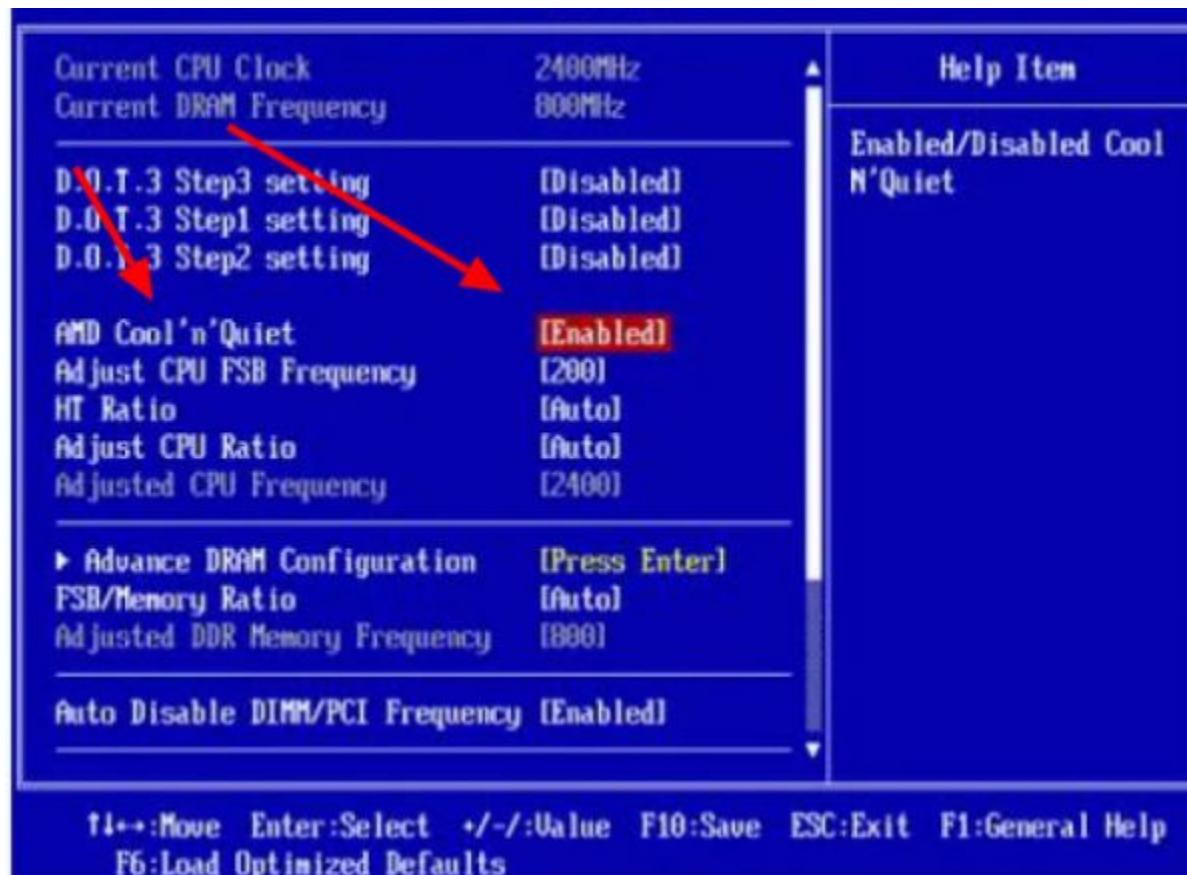
У интел - thermal monitor, AMD имеет аналогичные средства

В простое	При средней нагрузке	Под максимальной нагрузкой	Критическая
Около 35	Около 50	Около 70	80+

Конечные значения зависят от множества параметров.

Энергосбережение

- Cool'n'Quiet у AMD
- SpeedStep у intel



Антивирусная защита

Intel® Control-Flow Enforcement Technology (Intel CET)

INTEL CET = INDIRECT BRANCH TRACKING (IBT) + SHADOW STACK (SS)

INDIRECT BRANCH TRACKING (IBT)

IBT delivers indirect branch protection to defend against jump/call oriented programming (JOP/COP) attack methods.

```
<main>:  
: movq $0x4004fb, -8(%rbp)  
: mov -8(%rbp), %rdx  
: call *%rdx  
: retq
```

```
<foo>:  
: endbranch  
: add rax, rbx  
: retq
```

Intel CET will help prevent attackers from jumping to arbitrary addresses

SHADOW STACK (SS)

SS delivers return address protection to defend against return-oriented programming (ROP) attack methods.

```
STACK  
Return 1  
:  
Data  
:  
Return 2.1  
:  
Data
```

```
SHADOW STACK  
Return 1  
Return 2
```

Intel CET will help block call if return addresses on both stacks don't match

Intel CET helps protect against ROP/JOP/COP malware

Intel CET is built into the hardware microarchitecture and available across the family of products with that core. On Intel vPro® platforms with Intel® Hardware Shield, Intel CET further extends threat protection capabilities.

No product or component can be absolutely secure. © Intel Corporation. Intel, the Intel logo and other Intel marks are trademarks of Intel Corporation or its subsidiaries.

У интел:
Control-Flow
Enforcement
Technology

AMD Shadow Stack

Более сложное:
Защищенная шифрованная
виртуализация (SEV)